THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ERIC FLORENCE and AISHA BUNDAGE, on behalf of themselves and all others similarly situated,	)	
Plaintiffs,	)	No. 22 C 7210
v.	)	Judge Virginia M. Kendall
ORDER EXPRESS, INC.,	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

Plaintiffs Eric Florence and Aisha Bundage were customers of Defendant Order Express, Inc.'s money-services business. After a data breach, Plaintiffs' personal information appeared for sale on the dark web. Plaintiffs sued Order Express, bringing claims of negligence, breach of implied contract, and violation of the California Consumer Protection Act (CCPA). Order Express now moves to dismiss Plaintiffs' amended complaint for lack of standing and argues further that the CCPA claim is insufficiently pleaded. (Dkt. 17). For the reasons below, Order Express's motion is denied.

BACKGROUND

Unless otherwise noted, the following factual allegations are taken from Plaintiffs' Amended Class Action Complaint (Dkt. 15) and are assumed true for purposes of this motion. *W. Bend Mut. Ins. Co. v. Schumacher*, 844 F.3d 670, 675 (7th Cir. 2016); *Ctr. For Dermatology & Skin Cancer, Ltd. v. Burwell*, 770 F.3d 586, 588 (7th Cir. 2014).

Order Express is a money-services business, which collected personal identifying information—including names, social security numbers, and driver's license numbers—from over 63,000 customers. (Dkt. 15 ¶¶ 1–3). Order Express stored customers' personal identifying information on an unencrypted and internet-accessible network. (*Id.* at ¶ 4). By September 7, 2022, Order Express discovered an ongoing data breach, implicating the personal identifying information. (*Id.* at ¶¶ 5–6). Due to the breach, six gigabytes of customer data appeared for sale on the "dark web." (*Id.* at ¶¶ 7–10).[1] The data included names, addresses, phone numbers, order histories, social security numbers, identity documents, driver's licenses, payment information, "and much more." (*Id.* at ¶ 10). Reports emerged in October 2022 that the "CL0P" ransomware gang had orchestrated the attack on Order Express's network. (*Id.* at ¶ 7). One website stated that the stolen data was subject to a "[r]ansom deadline" of September 19, 2023. (*Id.* at ¶ 8).

Around December 15, 2022, Order Express began to notify state attorneys general and customers about the data breach. (*Id.* at ¶¶ 11–12). Order Express explained to customers that an "unknown party accessed parts of [its] computer network without authorization" and that their personal identifying information had been exposed. (*Id.* at ¶ 33). But Order Express's notices to customers and attorneys general did not disclose that an unauthorized actor had in fact acquired customers' personal identifying information. (*Id.* at ¶ 13). Nor did Order Express disclose that the personal identifying information was for sale on the dark web and subject to a ransom demand. (*Id.*)

[1] Plaintiffs' operative complaint does not define "dark web." (*See* Dkt. 15). The terms "dark web" or "darknet" describe "[w]ebsites and services, used esp[ecially] for criminal activity, which are hidden from standard search engines and allow owners and users to remain secret." *Dark Web*, Oxford English Dictionary (3d ed. 2021), https://www.oed.com/view/Entry/93164789; *Darknet*, *supra*, https://www.oed.com/view/Entry/93166091 ("Any of various covert networks on the internet allowing anonymous or encrypted communication, accessed using specific software, system configuration, or authorization, and often used for illegal commerce . . . .); *see also, e.g.*, *United States v. Kienast*, 907 F.3d 522, 526 (7th Cir. 2018).

Florence, a California resident, and Bundage, a Texas resident—both of whom had used Order Express to send or receive money before the data breach—were among the affected customers. (*Id.* at ¶¶ 21–22, 75, 83). Florence received a notice from Order Express stating that his driver's license number was subject to the data breach. (*Id.* at ¶¶ 34, 75). Order Express notified Bundage that her social security or tax identification numbers were exposed. (*Id.* at ¶ 83). After receiving the data-breach notice, Florence and Bundage attempted to mitigate the risks of the breach by verifying the notice's legitimacy and monitoring their accounts. (*Id.* at ¶¶ 77, 85). They spent time and money on credit monitoring, identity-theft insurance, scrutinizing bank and credit card statements and credit reports, and setting up fraud alerts. (*Id.* at ¶ 143). The exposure of their personal information in the data breach, Plaintiffs assert, has nonetheless left them vulnerable to "fraud, identify theft, and misuse" by unauthorized third parties or criminals. (*Id.* at ¶¶ 81, 89).

On the dark web, personal information sells for $40 to $200, and bank details sell for $50 to $200. (*Id.* at ¶ 64). Fraudulent uses of personal information include obtaining driver's licenses, government benefits, medical services, or housing. (*Id.* at ¶ 67). Identity thieves can also give false information to police. (*Id.*) Plaintiffs' stolen information is "difficult, if not impossible, to change." (*Id.* at ¶ 65). And fraudulent activity may not become apparent until years after a data breach. (*Id.* at ¶¶ 68–69). Order Express offered Plaintiffs two years of credit monitoring and identity-theft protection, which Plaintiffs allege is insufficient. (*Id.* at ¶¶ 71, 73).

Florence brought this putative class action on December 28, 2022. (Dkt. 1). In their Amended Class Action Complaint, Florence and Bundage allege negligence (Count I) and breach of implied contract (Count II), seeking declaratory and injunctive relief (Count III) in addition to damages. (Dkt. 15). Florence brings an additional claim under the CCPA, Cal. Civ. Code

§§ 1798.100, *et seq*. (*Id.*).[2] Order Express now moves to dismiss the amended complaint for lack of standing under Federal Rule of Civil Procedure 12(b)(1) and to dismiss Florence's CCPA claim under Rule 12(b)(6). (Dkt. 17).

LEGAL STANDARD

Rule 12(b)(1) motions "are meant to test the sufficiency of the complaint, not to decide the merits." *Ctr. for Dermatology & Skin Cancer*, 770 F.3d at 588. While the plaintiffs bear the burden of showing that subject-matter jurisdiction is proper, the Court accepts the well-pleaded factual allegations in the plaintiffs' complaint as true and draws reasonable inferences in their favor. *Id.* at 588–89. If the Court lacks subject-matter jurisdiction, it must dismiss the action without reaching the merits. *MAO-MSO Recovery II, LLC v. State Farm Mut. Auto. Ins. Co.*, 935 F.3d 573, 581 (7th Cir. 2019).

To survive a motion to dismiss under Rule 12(b)(6), the complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." *Kaminski v. Elite Staffing*, 23 F.4th 774, 776 (7th Cir. 2022) (quoting Fed. R. Civ. P. 8(a)(2)). The plaintiffs "must allege 'enough facts to state a claim that is plausible on its face.'" *Allen v. Brown Advisory, LLC*, 41 F.4th 843, 850 (7th Cir. 2022) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially plausible when the plaintiffs plead "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (quoting *Ashcroft v. Iqbal*, 566 U.S. 662, 678 (2009)). Again, the Court accepts the plaintiffs' well-pleaded

[2] Before bringing this suit, Florence gave Order Express written notice of its alleged violation of § 1798.150 of the CCPA. (*Id.* at ¶ 161; Dkt. 22 at 11). Order Express responded to the notice stating that it had cured any violations by enhancing its security measures. (Dkt. 22 at 12). Within 30 days of receiving the notice, Florence alleges, Order Express did not encrypt his personal identifying information or delete the information that it no longer needed to maintain on its internet-accessible network. (Dkt. 15 ¶¶ 162–63). Opposing Order Express's motion to dismiss, Florence has elaborated on the contents of its notice and Order Express's response—additional allegations which are consistent with the amended complaint, and which the Court may consider. *See Smith v. Dart*, 803 F.3d 304, 311 (7th Cir. 2015).

factual allegations as true, drawing reasonable inferences in their favor. *Id.* (citing *W. Bend*, 844 F.3d at 675).

DISCUSSION

I. Article III Standing

Article III of the Constitution limits federal jurisdiction to "cases" and "controversies." U.S. Const. art. III § 2; *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203 (2021). Thus, the party "invoking the power of a federal court must demonstrate standing to do so." *Hero v. Lake Cnty. Election Bd.*, 42 F.4th 768, 772 (7th Cir. 2022) (quoting *Hollingsworth v. Perry*, 570 U.S. 693, 704 (2013)). To have standing, a plaintiff must show: (1) an injury in fact; (2) traceable to the defendant; and (3) redressable by judicial relief. *Pierre v. Midland Credit Mgmt., Inc.*, 29 F.4th 934, 937 (7th Cir. 2022); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992). Plaintiffs need "standing for each claim that they press and for each form of relief that they seek." *TransUnion*, 141 S. Ct. at 2208. And in a putative class action, each named plaintiff must demonstrate "that they personally have been injured, not that injury has been suffered by other, unidentified members of the class." *Warth v. Seldin*, 422 U.S. 490, 502 (1975).

Important here, an adequate injury in fact is "concrete, particularized, and actual or imminent." *Ewing v. MED-1 Sols., LLC*, 24 F.4th 1146, 1151 (7th Cir. 2022). Although a concrete injury need not be tangible, it must be "real," rather than "abstract." *Id.* (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016)); *see also Markakos v. Medicredit, Inc.*, 997 F.3d 778, 781 (7th Cir. 2021) (noting that "a statutory violation alone" is not an injury in fact). Concreteness is essential: "No concrete harm, no standing." *Ewing*, 24 F.4th at 1151 (quoting *TransUnion*, 141 S. Ct. at 2200). Then, the actual-or-imminent element "ensure[s] that the alleged injury is not too speculative." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013). An injury is therefore

imminent if the threat of future harm is "certainly impending"; the mere possibility of a future injury is not enough. *Id.*

The Seventh Circuit considered concreteness and imminence in the data-breach context in *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015). There, customers sued a department store after hackers stole their credit card numbers—some which had already been fraudulently used. *Id.* at 690. The Court held that the not-yet-defrauded customers alleged imminent injuries because the exposure of their credit card numbers created an "objectively reasonable likelihood" of identity theft and fraudulent charges. *Id.* at 693 (quoting *Clapper*, 568 U.S. at 410). If not to make fraudulent charges or steal customers' identities, "[w]hy else would hackers break into a store's database and steal consumers' private information?" *Id.* "Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years." *Id.* at 694 (quotation omitted). Considering the "substantial risk" of identity theft, the customers' mitigation expenses—specifically, the costs of credit monitoring—reflected an additional concrete harm. *Id.*; *see also Clapper*, 568 U.S. at 414 n.5 (noting the existence of standing where "substantial risk" of harm "may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm"). Since the department store had offered credit monitoring and identity-theft protection to customers after the breach, it was reasonable for the customers to believe credit monitoring was a necessary expense. *Remijas*, 794 F.3d at 694.

Similarly, the Seventh Circuit held that standing was proper in *Lewert v. P.F. Chang's China Bistro, Inc.*, another credit card data-breach case. 819 F.3d 963, 967 (7th Cir. 2016). The *Lewert* plaintiffs, like the customers in *Remijas*, alleged imminent injuries because the theft of their credit card numbers subjected them to an "increased risk of fraudulent charges and identity theft." *Id.* at 967. One plaintiff had already suffered fraudulent charges, which his bank prevented

from going through. *Id.* Still, his time and effort spent resolving the fraudulent charges amounted to a concrete harm. *Id.* Another plaintiff—who had not yet suffered fraudulent charges or identity theft—alleged he spent time and effort spent monitoring credit card statements and other financial information to prevent those imminent future injuries. *Id.* That was a concrete harm too. *Id.* The plaintiffs' mitigation efforts were reasonable because hackers could use their stolen credit cards to open new cards in their names. *Id.* Plus, the defendant encouraged its customers to monitor their credit reports. *Id.*

Since *Remijas* and *Lewert*, the Supreme Court has clarified that a substantial risk of future harm can support standing only for "forward-looking, injunctive relief to prevent the harm from occurring." *TransUnion*, 141 S. Ct. at 2210 (citing *Clapper*, 568 U.S. at 414 n.5). Pursuing damages, however, requires a concrete harm that has already materialized. *Id.* at 2210–11; *see Pierre*, 29 F.4th at 938 ("A plaintiff seeking money damages has standing to sue in federal court only for harms that have in fact materialized."); *Ewing*, 24 F.4th at 1151 ("[A] risk of future harm is concrete only if the suit is for injunctive relief."). Still, *TransUnion* did not foreclose the possibility of concrete injuries arising from the risk of future harm. *See TransUnion*, 141 S. Ct. at 2211 & n.7. The mitigation costs in *Remijas* and *Lewert* would fall into that category.

The Supreme Court's opinion in *Spokeo, Inc. v. Robins* recognized that an intangible injury can be concrete if it has a "close relationship" to a traditionally recognized common-law harm. *Spokeo*, 578 U.S. at 340–41. A close relationship, the Court explained in *TransUnion LLC v. Ramirez*, "does not require an exact duplicate in American history and tradition." *TransUnion*, 141 S. Ct. at 2204; *Ewing*, 24 F.4th at 1151. Instead, the test is whether the plaintiff's injury has "a close historical or common-law analogue." *Ewing*, 24 F.4th at 1151 (quoting *TransUnion*, 141 S. Ct. at 2204). To measure concreteness, courts "look to both history and Congress's

judgment." *Pucillo v. Nat'l Credit Sys., Inc.*, 66 F.4th 634, 639 (7th Cir. 2023). Concrete intangible injuries "include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion." *TransUnion*, 141 S. Ct. at 2204 (citations omitted).

Against that backdrop, Plaintiffs argue that their (1) loss of privacy; (2) mitigation efforts; and (3) emotional injuries based on the threat of future harm are concrete injuries providing standing to seek both damages and injunctive relief. (Dkt. 22 at 3–10).

A. Loss of Privacy

Plaintiffs' alleged loss of privacy resulting from the data breach is a concrete injury in fact. The publication of Plaintiffs' sensitive personal information—including social security numbers, driver's license numbers, and tax identification numbers—has a close relationship to disclosure of private information, a common-law theory of harm. *See TransUnion*, 141 S. Ct. at 2204 (observing that disclosure of private information exemplifies a common-law analogue for a concrete harm); *Davis v. Fed. Election Comm'n*, 554 U.S. 724, 733 (2008) (holding that the plaintiff suffered a concrete harm by involuntarily disclosing that he spent personal funds on his election campaign).

At common law, disclosure of private information was one of four theories of wrongdoing under the umbrella of the tort of invasion of privacy—the other three theories being intrusion upon seclusion, appropriation of another's name or likeness, and publicity placing another in a false light. *Pucillo*, 66 F.4th at 639–40; Restatement (Second) of Torts § 652A (Am. L. Inst. 1977); *see, e.g.*, *Persinger v. Sw. Credit Sys., L.P.*, 20 F.4th 1184, 1193 (7th Cir. 2021) (holding unauthorized requests of a consumer's credit history are sufficiently close to intrusion upon seclusion); *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 462 (7th Cir. 2020) (holding unwanted text messages can cause harm analogous to intrusion upon seclusion). Disclosure of private information imposes liability where a defendant "gives publicity to a matter concerning the private life of another,"

where "the matter publicized is of a kind that . . . would be highly offensive to a reasonable person, and . . . is not of legitimate concern to the public." Restatement (Second) of Torts § 652D; *id.* cmt. b ("[T]here is no liability for giving publicity to facts about the plaintiff's life that are matters of public record," but "if the record is one not open to public inspection, as in the case of income tax returns, it is not public, and there is an invasion of privacy when it is made so."); *see also Am. C.L. Union of Ill. v. Alvarez*, 679 F.3d 583, 606 n.12 (7th Cir. 2012).

Plaintiffs allege that Order Express failed to prevent hackers from stealing and publishing their social security, driver's license, and tax identification numbers—information which a reasonable person would prefer to keep private. The resulting likelihood of fraud or identity theft makes the exposure of Plaintiffs' private information even more offensive. Their social security numbers and driver's license numbers, of course, are not of legitimate public concern.

Since disclosure of private information is a sufficiently close common-law analogue for Plaintiffs' alleged harm, the injury is concrete. *See TransUnion*, 141 S. Ct. at 2204; *see also, e.g.*, *Lueck v. Bureaus, Inc.*, 2021 WL 4264368, at *4 (N.D. Ill. Sept. 20, 2021) ("Certainly, a 'disclosure of private information' is a concrete, albeit intangible, harm—one that has been traditionally recognized as providing a basis for lawsuits in American courts." (quoting *TransUnion*, 141 S. Ct. at 2204)); *In re Clearview AI, Inc. Consumer Priv. Litig.*, 585 F. Supp. 3d 1111, 1126 (N.D. Ill. 2022) ("Plaintiffs have sufficiently alleged that defendants' disclosure of their private information without their consent caused them the concrete harm of violating their privacy interests in their biometric data."); *Dancel v. Groupon, Inc.*, 2018 WL 11195080, at *2 (N.D. Ill. Oct. 10, 2018) ("[T]he dissemination to a third party of information in which a person has a right to privacy is a sufficiently concrete injury for standing purposes."); *Krupa v. TIC Int'l Corp.*, 2023 WL 143140, at *2 (S.D. Ind. Jan. 10, 2023) ("Having one's social security number

stolen seems an obvious harm."); *cf. Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 910 (7th Cir. 2017) (holding no standing because the plaintiff had not alleged his personal information had been leaked or was at risk of being stolen).

After *TransUnion*, many federal courts have applied the close-relationship test to find concrete injuries in similar circumstances. *See, e.g.*, *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 155, 157–58 (3d Cir. 2022) ("[I]f the theory of injury is an unauthorized exposure of personally identifying information that results in an increased risk of identity theft or fraud, that harm is closely related to that contemplated by privacy torts that are 'well-ensconced in the fabric of American law.'" (quotation omitted)); *Wynne v. Audi of Am.*, 2022 WL 2916341, at *4–5 (N.D. Cal. July 25, 2022) (finding a concrete injury based on alleged theft of "sensitive personal information, including names, addresses, driver's license numbers, social security numbers, dates of birth, account and loan numbers, and tax identification numbers"); *Rand v. Travelers Indem. Co.*, 2022 WL 15523722, at *4–5 (S.D.N.Y. Oct. 27, 2022) (disclosure of "plaintiff's driver's license number and other [personal identifying information] to an unauthorized third party" was a concrete injury); *Perry v. Bay & Bay Transp. Servs., Inc.*, 2023 WL 171885, at *1, 5 (D. Minn. Jan. 12, 2023) (disclosure of name, address, date of birth, social security number, driver's license, and account information to cybercriminals was a concrete harm).

Conceding that social security numbers are sensitive information, Order Express argues that driver's license numbers are not, distinguishing Florence's alleged harm from Bundage's. (Dkt. 23 at 3). Even if a social security number is more sensitive than a driver's license number, Order Express ignores that the close-relationship test requires an analogy—not an "exact duplicate." *See TransUnion*, 141 S. Ct. at 2204. At this stage, it is enough that a reasonable person would wish to keep their driver's license number private, including because identity thieves can

put stolen driver's license numbers to fraudulent use. *See Clemens*, 48 F.4th at 155 n.5 ("[T]he exposure of the type of information that was alleged here—information employees would normally choose to keep to themselves and would reasonably not want to make publicly available—and the resulting substantial risk of identity theft or fraud is a harm that bears at least a 'close relationship' to harms traditionally recognized in privacy torts."). Several other courts have found the exposure of a driver's license number alone to be a concrete harm. *E.g.*, *Park v. Am. Fam. Life Ins. Co.*, 608 F. Supp. 3d 755, 757 (W.D. Wis. 2022); *In re USAA Data Sec. Litig.*, 2022 WL 3348527, at *5 (S.D.N.Y. Aug. 12, 2022); *Stallone v. Farmers Grp. Inc.*, 2022 WL 10091489, at *6–7 (D. Nev. Oct. 15, 2022). For now, both Plaintiffs' alleged harms are suitably concrete.

B. Mitigation Costs

Plaintiffs allege an additional concrete harm in the form of mitigation costs based on the threat of future harm. After a data breach, the risk of identity theft or fraud is "sufficiently immediate to justify mitigation efforts." *Lewert*, 819 F.3d at 967; *Remijas*, 794 F.3d at 694. The costs of mitigating an imminent risk of future harm can provide standing to support claims for both damages and injunctive relief, which is consistent with *TransUnion*. *See TransUnion*, 141 S. Ct. at 2211 & n.7 (holding certain plaintiffs lacked standing because they failed to show any harm independent of their exposure to an imminent risk—"that is, that they suffered some other injury . . . from the mere risk that their credit reports would be provided to third-party businesses"); *see also Clemens*, 48 F.4th at 155–56 (plaintiff had standing to pursue damages based on a "substantial risk of identity theft or fraud" because "the exposure to that substantial risk caused additional, currently felt concrete harms"); *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1263 (11th Cir. 2021) (holding plaintiffs' mitigation efforts after a data breach established a concrete harm). Other post-*TransUnion* data-breach decisions in the Seventh Circuit

have relied on *Remijas* and *Lewert* to find that mitigation costs based on imminent future harm amount to a concrete injury in fact. *E.g.*, *Linman v. Marten Transp. Ltd.*, 2023 WL 2562712, at *3 (W.D. Wis. Mar. 17, 2023); *Krupa*, 2023 WL 143140, at *2 n.1.

Order Express cites *Kim v. McDonald's USA, LLC*, which is distinguishable. 2022 WL 4482826 (N.D. Ill. Sept. 27, 2022). In *Kim*, the district court held that plaintiffs lacked standing to pursue claims arising from a data breach implicating their email addresses, phone numbers, and physical addresses. *Id.* at *5–8. Based on the exposure of that *non-sensitive* information, plaintiffs failed to allege that identity theft or phishing scams were "certainly impending." *Id.* at *5 (quoting *Clapper*, 568 U.S. at 409). In the absence of any imminent harm, the plaintiffs' mitigation expenses relied on "speculation about the 'unfettered choices made by independent actors not before the court.'" *Id.* at *6 (quoting *Clapper*, 568 U.S. at 414 n.5).

Unlike in *Kim*, Plaintiffs have alleged an imminent threat of identity theft and fraud due to the exposure of their social security and driver's license numbers. Based on the substantial risk of harm, Plaintiffs allege that they have spent time and money on credit monitoring and identity-theft insurance. *See Lewert*, 819 F.3d at 967. Underscoring the reasonableness of Plaintiffs' mitigation efforts is Order Express's offer to pay for two years of credit monitoring and identity-theft protection. *See Remijas*, 794 F.3d at 694; *Lewert*, 819 F.3d at 967; *see also Doe v. Fertility Ctrs. of Ill., S.C.*, 2022 WL 972295, at *2 (N.D. Ill. Mar. 31, 2022).

In sum, Plaintiffs have demonstrated actual and imminent concrete harms by alleging loss of privacy and mitigation costs based on the substantial risk of identity theft and fraud. These harms are traceable to the data breach, which Order Express failed to prevent, and redressable by this Court. The "standing inquiry remains open to review at all stages of the litigation," and Plaintiffs' burden to show standing will grow heavier as this litigation moves forward. *Persinger*,

20 F.4th at 1189. At this stage, Plaintiffs have standing to pursue their claims for damages and injunctive relief.

C. Emotional Harm

For completeness, the Court mentions Plaintiffs' last concrete-harm theory: they claim to have suffered emotional distress, anxiety, and annoyance based on the risk of future harm. But the Seventh Circuit has repeatedly rejected arguments in this vein. *See Pierre*, 29 F.4th at 939 (explaining that emotional distress based on a fear of future harm does not confer standing); *Wadsworth v. Kross, Lieberman & Stone, Inc.*, 12 F.4th 665, 668 (7th Cir. 2021) (anxiety and stress "are quintessential abstract harms"); *Pucillo*, 66 F.4th at 638 ("[B]eing 'concerned' and 'upset' . . . is not a concrete injury."); *Gunn v. Thrasher, Buschmann & Voelkel, P.C.*, 982 F.3d 1069, 1071 (7th Cir. 2020) (annoyance and intimidation are not enough); *Markakos*, 997 F.3d at 781 (confusion and aggravation are not concrete); *Brunett v. Convergent Outsourcing, Inc.*, 982 F.3d 1067, 1068–69 (7th Cir. 2020) (observing that if confusion were a concrete harm, "everyone would have standing to litigate about everything"); *Pennell v. Glob. Tr. Mgmt., LLC*, 990 F.3d 1041, 1045 (7th Cir. 2021) ("Nor does stress by itself with no physical manifestations and no qualified medical diagnosis amount to a concrete harm."). Plaintiffs have not shown that their "emotional response led to actionable injury." *Pucillo*, 66 F.4th at 639. Unlike Plaintiffs' loss of privacy and mitigation costs, their emotional harms are not concrete.

II. California Consumer Privacy Act (Count IV)

Order Express next contends that Florence has failed to state a claim under the CCPA. (Dkt. 18 at 11–13). To state a claim under the CCPA, the plaintiff must allege that the defendant's failure to implement reasonable security measures allowed third parties to access and steal his

personal information. Cal. Civ. Code § 1798.150(a)(1); *In re Arthur J. Gallagher Data Breach Litig.*, 2022 WL 435092, at *11 (N.D. Ill. Sept. 28, 2022).[3]

Order Express first argues that § 1798.145(e) exempts it from liability under the CCPA. Section 1798.145(e) states that the CCPA:

> shall not apply to personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act . . . , and implementing regulations, or the California Financial Information Privacy Act . . . , or the federal Farm Credit Act of 1971 . . . . *This subdivision shall not apply to Section 1798.150*.

Cal. Civ. Code § 1798.145(e) (emphasis added). On its face, the exemption does not apply to § 1798.150—the Section under which Florence brings his claim.

Second, Order Express argues that the CCPA's notice-and-cure provision bars Florence's claim. To recover statutory damages under the CCPA, § 1798.150(b) requires consumers, before suing, to provide the defendant with 30-days' written notice identifying the specific provisions the defendant allegedly violated. Cal. Civ. Code § 1798.150(b); *Griffey v. Magellan Health Inc.*, 2022 WL 1811165, at *6 (D. Ariz. June 2, 2022). The consumer cannot pursue statutory damages if "the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur." Cal. Civ. Code § 1798.150(b); *In re Waste Mgmt. Data Breach Litig.*, 2022 WL 561734, at *6 (S.D.N.Y. Feb. 24, 2022). But "[t]he implementation and maintenance of reasonable security procedures and practices . . . following a breach does not constitute a cure with respect to that breach." Cal. Civ. Code § 1798.150(b).

---

[3] The CCPA provides a cause of action for:

> [a]ny consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.

Cal Civ. Code § 1798.150(a)(1).

Florence alleges he sent Order Express a notice identifying its alleged violation of § 1798.150. In Order Express's response, it claimed to have enhanced its security measures, which Florence argues, amounted to the "implementation and maintenance of reasonable security procedures and practices"—rather than a cure—under § 1798.150(b). Florence alleges further that Order Express's response to his notice did not explain how its enhanced security measures actually cured the alleged CCPA violation. Order Express did not encrypt Florence's personal identifying information or delete the information it no longer needed to maintain on its internet-accessible network. Nor has Order Express expanded on its bare assertion in the motion to dismiss that it "cured all alleged violations within the requisite time period." (Dkt. 18 at 13). Accordingly, Florence has stated a claim under the CCPA.

CONCLUSION

For the reasons above, Order Express's motion to dismiss [17] is denied.

Virginia M. Kendall
United States District Judge

Date: May 23, 2023